REMARKS

Claims 2 - 5, 7 - 10, and 27 - 30 are pending. Claims 1, 6, and 11 - 26 have been cancelled. Claims 2 - 5 and 7 - 10 have been amended. No new matter has been introduced. Reexamination and reconsideration of the application are respectfully requested.

In the November 23, 2004 Office Action, the Examiner identified that the applicant, in a telephonic conversation, had provisionally elected to prosecute the invention of group I, claims 1 - 14. The applicant affirms this election of the group 1 claims, claims 1 - 14. Claims 15- 26 have been cancelled, without prejudice.

The Examiner objected to the drawings under 37 C.F.R. 1.84(p)(5) because they include reference characters not included in the description. The applicant has amended Figs. 3(a) and 3(b) as illustrated in the included replacement drawings. Applicant respectfully requests that the objection to the drawings be withdrawn.

The Examiner objected to claims 1 - 2, 6 - 7, and 12 for informalities. The applicant has cancelled claims 1, 6, and 12. The applicant has amended claims 2 and 7 to address the Examiner's concern.

The Examiner rejected claims 1 - 2, 6 - 7, and 11 - 12 under 35 U.S.C. § 103(a) as being unpatentable over the RFC 2093 - Group Key Management Protocol Specification to Haney ("the Harney reference") in view of a "Handbook of Applied Cryptography" by Menezes et al. ("the Menezes reference"). The Examiner rejected claims 3, 5, 8, 10, and 13 under 35 U.S.C. § 103(a) as being unpatentable over the Harney reference in view of the Menezes reference and further in view of "Enclaves: Enabling Secure Collaboration Over the Internet" by Gong ("the Gong reference"). The

Examiner rejected claims 4, 9, and 14 under 35 U.S.C. § 103(a) as being unpatentable over the Harney reference in view of the Menezes reference and further in view of WIPO Publication No. 01/13201 A2 to Waldman ("the Waldman reference"). These rejections are respectfully traversed in so far as they are applicable to the presently pending claims.

Independent claim 27 distinguishes over the cited references. Independent claim 27 recites:

> A method for creating a semi-private peer network, comprising:
> sending an encrypted key from a connecting member peer node to a plurality of member peer nodes to connect to the plurality of peer nodes, the plurality of peer nodes corresponding to a plurality of addresses, respectively, of a connection list of addresses;
> **establishing a connection between the connecting member peer node and responsive nodes of the plurality of member peer nodes that successfully decrypt the encrypted key because the responsive nodes had been previously supplied with the encrypted key; and**
> **updating an active connection list in the connecting member peer node listing the responsive nodes that successfully decrypt the encrypted key.**

The Harney reference does not disclose, teach, or suggest the method for creating a semi-private peer network of claim 27. The Examiner states that the Harney reference discloses sending a shared secret key from a connecting member peer mode of the semi-private peer network to the one or more member peer nodes. *(Office Action, page 5)*. The Harney reference is directed to a group key management protocol and proposes a protocol to create grouped symmetric keys and distribute them amongst communicating peers. Specifically, the Harney reference discloses that a general controller cooperates with a first member to create a first group key and then to send the group controller identity, the group identity, the group member identities, group

permissions, and group permissions to the first member. After this occurs the other group members must get the group keys before the group is fully operational. The other group member initialization includes sending a key packet including the keys, group identity, general controller (GC) identity, group member identities, group permissions, and group re-key interval to the other members. *(Harney, Sections 6.1.2 and 6.1.3)*.

This is not the same as a method of creating a semi-private peer network including **establishing a connection between the connecting member peer node and responsive nodes of the member peer nodes that successfully decrypt the encrypted key because the responsive nodes had previously received the encrypted key; and updating an active connection list in the connecting member peer node listing the responsive nodes that successfully decrypt the encrypted key.** Instead, the Harney reference discloses only the transferring of keys, and not establishing a connection between the connecting member peer node and the responsive nodes, as recited in claim 27. Further, in the Harney reference, the first member and other members had not previously received the encrypted key because the keys are being generated in the interaction between the general controller (GC) and the first member and then between the other members and the GC. The Harney reference also never discloses updating an active connection list in the connecting member peer node, which lists **the responsive nodes of member peer nodes that successfully decrypt the encrypted key**. Accordingly, claim 27 distinguishes over the Harney reference.

The Menezes reference does not make up for the deficiencies of the Harney

reference. The Examiner utilizes the Menezes reference to disclose generating a session key encrypted using the shared symmetric key from a connecting node. *(Office Action, page 5)*. The generation of a session key encrypted using the shared symmetric key is not a limitation that is claimed in the method of claim 27. Accordingly, applicant respectfully submits that claim 27 distinguishes over the Harney / Menezes reference combination.

The Gong reference does not make up for the deficiencies of the Harney and the Menezes references. The Examiner states that the Gong reference discloses associating TCP port identifiers with the TCP/IP addresses. *(Office Action, page 6)*. The Examiner states that the Gong reference also discloses associating each member peer node with a particular port number limits the establishing a connection to the one or more peer nodes as an already connected member peer node. *(Office Action, page 6)*.

Specifically, the Gong reference discloses if a member wants to join the group, the member makes a request to the leader about whether they can join the group. The leader checks the validity of the request messages and if satisfied, checks to see if the user can be admitted. If yes, the group leader returns the group key for communicating among group members. When a user is admitted to the group, the leader arranges a state transfer (including the group membership list and references of all shared resources such as text files) to update the user. *(Gong, page 570, 1st column - 3rd full paragraph and 2nd column - 1st full paragraph)*.

This is not the same as a method for creating a semi private peer network including **establishing a connection between the connecting member peer node**

and responsive nodes of the plurality of member peer nodes that successfully decrypt the encrypted key because the responsive nodes had been previously supplied with the encrypted key; and updating an active connection list in the connecting member peer node listing the responsive nodes that successfully decrypt the encrypted key. It is not the same because in the Gong reference, a user requests from a group leader whether or not they can join the group and there is no establishing of a **connection between responsive nodes that successfully encrypt the decrypted key**. In other words, the Gong reference requires communication with a group leader before beginning group communication and thus is not having a **connecting node send out requests to a plurality of member peer nodes**, as recited in claim 27. Further, the Gong reference does not disclose **updating an active connection list in the connecting member peer node listing the responsive nodes plurality of member peer nodes that successfully decrypt the encrypted key** because in the Gong reference, the leader transfers a group membership list after the user is admitted to the group. Accordingly, applicant respectfully submits that claim 27 distinguishes over the Gong reference, alone or in combination, with the Harney and the Menezes references.

The Waldman reference does not make up for the deficiencies of the Harvey, Menezes, and Gong references. The Examiner states that the Waldman reference discloses associating an encrypted password with each peer member and that the password meets the limitation of a key. *(Office Action, page 7)*. Assuming, *arguendo*, that the Waldman reference discloses all that the Examiner states that it does, the Waldman reference does not disclose a method of creating a semi-private peer network

including **establishing a connection between the connecting member peer node and responsive nodes of the plurality of member peer nodes that successfully decrypt the encrypted key because the responsive nodes had been previously supplied with the encrypted key; and updating an active connection list in the connecting member peer node listing the responsive nodes that successfully decrypt the encrypted key.** Accordingly, applicant respectfully submits that claim 27 distinguishes over the Harney / Menezes / Gong / Waldman reference combination.

Independent claim 29 recites limitations similar to claim 27. Accordingly, applicant respectfully submits that claim 29 distinguishes over the Harney / Menezes / Gong / Waldman reference combination for reasons similar to those discussed above in regard to claim 27.

Claims 2 - 5, 7 - 10, 28, and 30 depend, directly or indirectly on independent claims 27 and 29. Accordingly, applicant respectfully submits that claims 2 - 5, 7 - 10, 28, and 30 distinguish over the Harney / Menezes / Gong / Waldman reference combination for the same reasons as those discussed above in regard to claim 27.

Claim 28 further distinguishes over the cited references. Claim 28 recites:

> The method of claim 27, wherein the connecting member peer node **has a predetermined limit of responsive nodes of the plurality of member peer nodes that the connecting member peer node is connected to and does not exceed the predetermined limit**.

None of the Harney / Menezes / Gong / Waldman references disclose that connecting member peer node has a predetermined limit of responsive nodes to which the connecting member peer node is connected. There is no discussion of a limit. Accordingly, applicant respectfully submits that claim 28 further distinguishes over the Harney / Menezes / Gong / Waldman reference combination.

Claim 30 recites limitations similar to claim 28. Accordingly, applicant respectfully submit that claim 30 distinguishes over the Harney / Menezes / Gong / Waldman reference combination.

Claim 5 further distinguishes over the cited references. Claim 5 recites:

> The method of claim 27, wherein **the connecting member peer node cannot be connected to a same set of member peer nodes as an already connected member peer node of the plurality of member peer nodes.**

The Examiner states that the Harney reference does not disclose limiting establishing a connection to the one or other member peer nodes that are connected to an already connected member peer node. The applicant agrees with the Examiner. The Menezes reference also does not disclose the above-highlighted limitation because there is no discussion of limiting a number of connections. Accordingly, applicant respectfully submits that claim 5 further distinguishes over the Harney / Menezes reference combination.

The Examiner states that the Gong reference discloses associating each member peer node with a port number and therefore limits establishing a connection to the one or more member peer nodes that are not connected to a same set of member peer nodes as an already connected peer node. *(Office Action, page 6)*. The applicants are confused by the Examiner's statement. The Gong reference discloses assigning a user a specific port number so that the user cannot have more than one instance that is active in the group. *(Gong, page 370)*. This is not the same as **the connecting member peer node not being connected to a same set of member peer nodes as an already connected member peer node of the plurality of member peer nodes**. It is not the same because in the Gong reference, there is only

discussion of the a one-to-one relationship between a port and a group member while claim 5, as amended, requires that **a same set of connecting peer nodes cannot be connected to both a connecting member peer node and an already connected member peer mode**. Accordingly, applicant respectfully submits that claim 5, as amended, further distinguishes over the Gong reference, alone or in combination with the Harney and Menezes reference.

Claim 10, as amended, recites limitations similar to claim 5, as amended. Accordingly, applicant respectfully submits that claim 10, as amended, further distinguishes over the Harney, Menezes, and Gong references, alone or in combination, for reasons similar to those discussed above in regard to claim 5, as amended.

///

///

///

///

///

///

///

///

///

///

///

///

///

Applicant believes that the claims are in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Respectfully submitted,

PILLSBURY WINTHROP LLP

Date: February 23, 2005

By: _____
Mark R. Kendrick
Registration No. 48,468
Attorney for Applicant(s)

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033

IN THE DRAWINGS

Figures 3(a) and 3(b) have been amended as shown in the replacement drawings.